นโยบายการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ ความปลอดภัยทางไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล

1. เจตนารมณ์ของนโยบาย

บริษัท โรงพยาบาลพระรามเก้า จำกัด (มหาชน) (“บริษัท” หรือ “โรงพยาบาล”) ให้ความสำคัญอย่างยิ่งต่อการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ ความปลอดภัยทางไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และความต่อเนื่องในการให้บริการทางการแพทย์ เนื่องจากข้อมูลสุขภาพ ข้อมูลผู้ป่วย ข้อมูลบุคลากร ข้อมูลทางธุรกิจ และระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเป็นทรัพยากรสำคัญที่มีผลโดยตรงต่อความปลอดภัยของผู้ป่วย คุณภาพการให้บริการ ความเชื่อมั่นของผู้มีส่วนได้เสีย และความต่อเนื่องในการดำเนินธุรกิจ

โรงพยาบาลจึงกำหนดนโยบายฉบับนี้ขึ้นเพื่อเป็นกรอบการเปิดเผยข้อมูลต่อสาธารณะเกี่ยวกับการบริหารจัดการความเสี่ยงด้านสารสนเทศและไซเบอร์ โดยอ้างอิงจากนโยบายและโปรแกรมภายในของโรงพยาบาล ได้แก่ นโยบายความมั่นคงปลอดภัยทางไซเบอร์ นโยบายการจัดการและการรักษาความปลอดภัยของข้อมูลสารสนเทศ นโยบายการรักษาความมั่นคงความปลอดภัยของข้อมูลในระบบเทคโนโลยีสารสนเทศ และโปรแกรมการตอบสนองการโจมตีทางไซเบอร์

นโยบายภายในของโรงพยาบาลกำหนดให้มีมาตรการด้าน Cybersecurity ที่เหมาะสม มีการประเมินความเสี่ยงด้าน Cybersecurity เป็นประจำทุกปี และมีการทดสอบแผนอย่างน้อยปีละ 1 ครั้ง โดยครอบคลุมพนักงาน คู่สัญญา บุคคลที่สาม และระบบเทคโนโลยีสารสนเทศทั้งหมดของโรงพยาบาล

2. ขอบเขตของนโยบาย

นโยบายฉบับนี้ครอบคลุมการกำกับดูแลและการบริหารจัดการในประเด็นสำคัญ ดังต่อไปนี้

1. ความมั่นคงปลอดภัยสารสนเทศ
2. ความปลอดภัยทางไซเบอร์
3. การคุ้มครองข้อมูลส่วนบุคคลและข้อมูลสุขภาพของผู้ป่วย
4. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ
5. การจำแนกประเภทข้อมูลและการรักษาความลับของข้อมูล
6. การสำรองข้อมูล การกู้คืนข้อมูล และความต่อเนื่องในการให้บริการ
7. การบริหารจัดการผู้ให้บริการภายนอกและบุคคลที่สามที่เกี่ยวข้องกับระบบสารสนเทศ
8. การเฝ้าระวัง การตรวจสอบ และการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
9. การอบรมและสร้างความตระหนักรู้แก่บุคลากร
10. การทบทวนและปรับปรุงนโยบายอย่างต่อเนื่อง

3. หลักการกำกับดูแล

โรงพยาบาลกำหนดให้การกำกับดูแลด้านสารสนเทศและไซเบอร์เป็นส่วนหนึ่งของระบบบริหารความเสี่ยงองค์กร โดยมีการกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้บริหาร หน่วยงานเทคโนโลยีสารสนเทศ หน่วยงานคุณภาพ บุคลากร ผู้ให้บริการ และบุคคลที่สามที่เกี่ยวข้องอย่างเหมาะสม

โรงพยาบาลจัดให้มีการติดตามสถานการณ์ภัยคุกคามทางไซเบอร์ทั้งในประเทศและต่างประเทศ รวมถึงความก้าวหน้าทางเทคโนโลยี เพื่อนำมาประเมินความเสี่ยงและปรับปรุงมาตรการป้องกันอย่างต่อเนื่อง นโยบายภายในยังกำหนดบทบาทของผู้บริหารและคณะกรรมการที่เกี่ยวข้องในการรับทราบนโยบาย ติดตามสถานการณ์ และให้คำแนะนำต่อฝ่ายบริหารโรงพยาบาลในประเด็นด้าน Cybersecurity

4. การบริหารความเสี่ยงด้านสารสนเทศและไซเบอร์

โรงพยาบาลจัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยทางไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อระบุ ประเมิน จัดลำดับความสำคัญ และกำหนดแผนลดความเสี่ยงที่เหมาะสม

การบริหารความเสี่ยงครอบคลุมทั้งความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล การโจมตีทางไซเบอร์ การหยุดชะงักของระบบสารสนเทศ ความเสี่ยงจากผู้ให้บริการภายนอก ความเสี่ยงจากอุปกรณ์เคลื่อนที่ และความเสี่ยงที่อาจกระทบต่อความต่อเนื่องในการให้บริการผู้ป่วย

นโยบายการจัดการและการรักษาความปลอดภัยของข้อมูลสารสนเทศของโรงพยาบาลกำหนดให้มีการประเมินความเสี่ยงด้านความปลอดภัยข้อมูลประจำปีทั่วทั้งองค์กร รวมถึงการจัดลำดับความเสี่ยงและจัดทำแผนงานลดความเสี่ยง

5. การจำแนกประเภทข้อมูลและการรักษาความลับ

โรงพยาบาลกำหนดแนวทางการจำแนกประเภทข้อมูลตามระดับความสำคัญ ความอ่อนไหว และข้อกำหนดด้านกฎหมาย โดยครอบคลุมข้อมูลผู้ป่วย ข้อมูลสุขภาพ ข้อมูลบุคลากร ข้อมูลทางการเงิน ข้อมูลการบริหาร ข้อมูลคุณภาพ ข้อมูลเหตุการณ์ไม่พึงประสงค์ ข้อมูลร้องเรียน และข้อมูลอื่นที่เกี่ยวข้องกับการดำเนินงานของโรงพยาบาล

ข้อมูลที่มีความอ่อนไหวหรือเป็นความลับจะได้รับการปกป้องด้วยมาตรการที่เหมาะสม เช่น การจำกัดสิทธิการเข้าถึง การจัดเก็บอย่างปลอดภัย การกำหนดผู้มีอำนาจอนุมัติ การควบคุมการเปิดเผยข้อมูล และการทำลายข้อมูลตามระยะเวลาที่กำหนด

เอกสาร HP-MOI-03 มีรายละเอียดการจำแนกข้อมูลของโรงพยาบาล เช่น ข้อมูลทางการเงิน ข้อมูลพนักงาน ข้อมูลงานคุณภาพ ข้อมูล Incident Report ข้อร้องเรียนของผู้ป่วย และข้อมูลที่ต้องจำกัดการเข้าถึงเฉพาะผู้เกี่ยวข้อง

6. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

โรงพยาบาลกำหนดให้มีการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศตามหลักความจำเป็นในการใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน โดยบุคลากร ผู้ให้บริการ และบุคคลที่สามจะได้รับสิทธิเข้าถึงเฉพาะข้อมูลหรือระบบที่จำเป็นต่อการปฏิบัติงานเท่านั้น

การบริหารสิทธิการเข้าถึงครอบคลุมการขออนุมัติสิทธิ การกำหนดบทบาทผู้ใช้งาน การทบทวนสิทธิ การยกเลิกสิทธิเมื่อสิ้นสุดหน้าที่หรือสัญญา และการควบคุมการเข้าถึงพื้นที่หรือระบบที่มีความสำคัญ

โรงพยาบาลมีมาตรการควบคุมการเข้าถึงทางกายภาพและทางระบบเทคโนโลยีสารสนเทศ รวมถึงข้อกำหนดเกี่ยวกับการพิสูจน์ตัวตน การรักษาความลับของรหัสผ่าน และการแจ้งเหตุเมื่อพบความผิดปกติของการใช้งาน

7. การคุ้มครองข้อมูลส่วนบุคคลและข้อมูลผู้ป่วย

โรงพยาบาลตระหนักว่าข้อมูลส่วนบุคคลและข้อมูลสุขภาพของผู้ป่วยเป็นข้อมูลที่มีความอ่อนไหวสูง จึงกำหนดให้มีมาตรการคุ้มครองข้อมูลดังกล่าวให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายที่เกี่ยวข้องกับการให้บริการทางการแพทย์ และหลักจริยธรรมของวิชาชีพ

โรงพยาบาลมุ่งมั่นที่จะรักษาความลับ ความถูกต้อง ความครบถ้วน และความพร้อมใช้ของข้อมูลผู้ป่วย โดยจำกัดการเข้าถึงเฉพาะผู้ที่มีหน้าที่เกี่ยวข้อง จัดให้มีแนวทางการใช้ การส่งต่อ การจัดเก็บ การขอข้อมูล การเปิดเผย และการทำลายข้อมูลอย่างเหมาะสม

8. การปกป้องระบบสารสนเทศและโครงสร้างพื้นฐานสำคัญ

โรงพยาบาลจัดให้มีมาตรการป้องกันและควบคุมความปลอดภัยของระบบสารสนเทศ เครือข่าย อุปกรณ์คอมพิวเตอร์ อุปกรณ์เคลื่อนที่ ระบบเวชระเบียนอิเล็กทรอนิกส์ ระบบสนับสนุนการรักษาพยาบาล และอุปกรณ์ทางการแพทย์ที่เชื่อมต่อกับระบบสารสนเทศของโรงพยาบาล

มาตรการดังกล่าวรวมถึงการควบคุมระบบเครือข่าย การป้องกันมัลแวร์ การควบคุมอุปกรณ์จากภายนอก การเข้ารหัสข้อมูลตามความเหมาะสม การรักษาความปลอดภัยของอุปกรณ์เคลื่อนที่ การสำรองข้อมูล การทดสอบระบบ และการติดตามเฝ้าระวังเหตุการณ์ผิดปกติ

นโยบายภายในของโรงพยาบาลระบุถึงการปกป้องข้อมูล ระบบเครือข่าย และอุปกรณ์ทางการแพทย์จากการเข้าถึงโดยไม่ได้รับอนุญาต การโจมตีทางไซเบอร์ และการละเมิดข้อมูลที่อาจกระทบต่อความปลอดภัยของผู้ป่วย ความต่อเนื่องของบริการ และความลับของข้อมูล

9. การบริหารจัดการผู้ให้บริการภายนอกและบุคคลที่สาม

โรงพยาบาลกำหนดให้ผู้ให้บริการภายนอก คู่สัญญา ผู้ติดตั้งระบบ ผู้ดูแลระบบ ผู้รับบำรุงรักษา และบุคคลที่สามที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ การรักษาความลับ และการคุ้มครองข้อมูลของโรงพยาบาล

การเข้าถึงระบบ ข้อมูล หรือพื้นที่สำคัญของโรงพยาบาลโดยบุคคลภายนอกต้องอยู่ภายใต้การอนุมัติ การควบคุม และการบันทึกตามแนวทางที่โรงพยาบาลกำหนด ทั้งนี้เพื่อป้องกันความเสี่ยงจากการเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

เอกสาร HP-MOI-15 ระบุแนวทางควบคุมการเข้าถึงพื้นที่สำคัญ เช่น Data Center โดยผู้ขาย ผู้ติดตั้งระบบ ผู้เชี่ยวชาญจากภายนอก หรือบุคคลภายนอกต้องได้รับการควบคุมและบันทึกการเข้าออกตามที่กำหนด

10. การสำรองข้อมูล การกู้คืนข้อมูล และความต่อเนื่องทางธุรกิจ

โรงพยาบาลจัดให้มีมาตรการสำรองข้อมูล การกู้คืนข้อมูล และแผนรองรับการหยุดชะงักของระบบสารสนเทศ เพื่อสนับสนุนความต่อเนื่องในการให้บริการผู้ป่วยและลดผลกระทบจากเหตุการณ์ไม่คาดคิด เช่น ระบบสารสนเทศขัดข้อง ภัยคุกคามทางไซเบอร์ ภัยพิบัติ หรือเหตุการณ์ที่ส่งผลกระทบต่อความพร้อมใช้ของระบบ

โรงพยาบาลมีการทดสอบและทบทวนแผนตอบสนองต่อการหยุดทำงานของระบบข้อมูลทั้งกรณีที่วางแผนไว้และไม่ได้วางแผนไว้อย่างน้อยปีละ 1 ครั้ง เพื่อปรับปรุงความพร้อมและความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ

11. การตอบสนองต่อเหตุการณ์ด้านไซเบอร์

โรงพยาบาลกำหนดโปรแกรมการตอบสนองการโจมตีทางไซเบอร์ เพื่อให้มีแนวทางปฏิบัติที่ชัดเจน ทันต่อเหตุการณ์ และสอดคล้องกับความสำคัญของการให้บริการทางการแพทย์ โดยมุ่งเน้นการควบคุมภัยคุกคาม การลดผลกระทบ การรักษาความต่อเนื่องของบริการผู้ป่วย การกู้คืนระบบ และการป้องกันการเกิดเหตุซ้ำ

หลักการตอบสนองต่อเหตุการณ์ด้านไซเบอร์ของโรงพยาบาล ได้แก่

1. ควบคุมและกักกันภัยคุกคามโดยเร็ว
2. ใช้แผนรองรับการหยุดทำงานของระบบสารสนเทศเมื่อจำเป็น
3. ให้ความสำคัญกับความปลอดภัยของผู้ป่วยและความต่อเนื่องของบริการทางการแพทย์
4. กู้คืนระบบและข้อมูลตามแผนที่กำหนด
5. วิเคราะห์สาเหตุและช่องโหว่หลังเกิดเหตุ
6. กำหนดมาตรการป้องกันการเกิดเหตุซ้ำ
7. ทบทวนบทเรียนหลังเหตุการณ์เพื่อปรับปรุงระบบควบคุม

โปรแกรมการตอบสนองการโจมตีทางไซเบอร์ของโรงพยาบาลระบุวัตถุประสงค์เพื่อให้มั่นใจในความพร้อมใช้ของระบบสารสนเทศ ความสมบูรณ์ของข้อมูล ความต่อเนื่องทางธุรกิจ และเพื่อให้บุคลากรเข้าใจหน้าที่ของตนเองเมื่อเกิดเหตุการณ์โจมตีทางไซเบอร์

12. การฝึกอบรมและการสร้างความตระหนักรู้

โรงพยาบาลจัดให้มีการอบรมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ ความปลอดภัยทางไซเบอร์ การใช้ข้อมูลอย่างเหมาะสม และการคุ้มครองข้อมูลส่วนบุคคลให้แก่บุคลากรที่เกี่ยวข้อง ทั้งในช่วงเริ่มงานและการทบทวนตามรอบระยะเวลาที่เหมาะสม

การอบรมครอบคลุมการใช้ระบบสารสนเทศ การรักษาความลับของข้อมูล การป้องกันภัยคุกคามทางไซเบอร์ การระมัดระวังการหลอกลวงทางอิเล็กทรอนิกส์ การรายงานเหตุผิดปกติ และบทบาทของบุคลากรในการปกป้องข้อมูลของผู้ป่วยและโรงพยาบาล

นโยบาย HP-MOI-03 ระบุให้มีการฝึกอบรมเกี่ยวกับระบบสารสนเทศ ความปลอดภัยของสารสนเทศ และหลักการใช้และการจัดการสารสนเทศ รวมถึงการใช้เวชระเบียนอิเล็กทรอนิกส์ตามหน้าที่ความรับผิดชอบให้กับบุคลากรใหม่และทบทวนความรู้ให้บุคลากรเดิมอย่างน้อยทุกปี

13. การติดตาม ตรวจสอบ และปรับปรุงอย่างต่อเนื่อง

โรงพยาบาลกำหนดให้มีการติดตาม เฝ้าระวัง ตรวจสอบ และทบทวนมาตรการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์อย่างต่อเนื่อง เพื่อให้มั่นใจว่ามาตรการควบคุมยังคงมีประสิทธิผลและสอดคล้องกับความเสี่ยงที่เปลี่ยนแปลงไป

โรงพยาบาลมีการทบทวนเหตุการณ์ผิดปกติ การตรวจสอบช่องโหว่ การติดตามภัยคุกคาม การประเมินผลการทดสอบแผน และการกำหนดมาตรการปรับปรุงเพื่อเพิ่มประสิทธิภาพของระบบการควบคุม

14. การเปิดเผยข้อมูลและข้อจำกัดด้านความมั่นคงปลอดภัย

โรงพยาบาลเปิดเผยนโยบายฉบับนี้เพื่อแสดงถึงกรอบการกำกับดูแลและการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ความปลอดภัยทางไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลต่อผู้มีส่วนได้เสีย

อย่างไรก็ตาม เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและข้อมูลสำคัญของโรงพยาบาล โรงพยาบาลจะไม่เปิดเผยรายละเอียดเชิงเทคนิค รายละเอียดโครงสร้างระบบ ขั้นตอนตอบสนองเหตุการณ์เชิงปฏิบัติการ รายละเอียดระบบสำรองข้อมูล ระยะเวลาการกู้คืนรายระบบ ช่องทาง escalation ภายใน รายชื่อผู้รับผิดชอบเชิงปฏิบัติการ หรือข้อมูลอื่นใดที่อาจเพิ่มความเสี่ยงด้านความปลอดภัยขององค์กร

15. การทบทวนนโยบาย

โรงพยาบาลจะทบทวนนโยบายฉบับนี้ตามรอบระยะเวลาที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น การเปลี่ยนแปลงของกฎหมาย มาตรฐานสากล ความเสี่ยงด้านไซเบอร์ เทคโนโลยี ระบบสารสนเทศ หรือโครงสร้างการกำกับดูแลขององค์กร เพื่อให้มั่นใจว่านโยบายยังคงเหมาะสม เพียงพอ และมีประสิทธิผล